Six Ways to Improve Your Network Security with SD-WAN

Brought to you by Silver Peak

Making broadband internet secure for the enterprise

Geographically distributed enterprises are embracing software-defined wide area networks (SD-WANs) at an accelerating pace. Why? Because SD-WANs not only dramatically lower costs, reduce complexity, and make branch communications more secure, they help businesses become more agile and responsive.

How does an SD-WAN solution do this? By enabling companies to use multiple forms of connectivity, including lower-cost broadband internet services, delivering significant CAPEX and OPEX savings while improving performance across the WAN. While a traditional WAN can take weeks or even months to spin up, an SD-WAN that includes broadband can be online within hours.

However, it takes the right SD-WAN solution to make broadband internet services secure enough for the enterprise. Read on to learn about six ways to use a secure SD-WAN solution to improve network security and compliance.

Enormous SD-WAN growth

According to market research firm IDC, the SD-WAN market is projected to see a 90% compound annual growth rate from 2015 to 2020.

Source: IDC, "IDC Forecasts Strong Growth for Software-Defined WAN as Enterprises Seek to Optimize Their Cloud Strategies," March 24, 2016.

#1

Safely use broadband internet services for cost-effective transport

The Internet has historically been too insecure for enterprise WAN use. That's why cloud-based application traffic is often backhauled from the branch across expansive multiprotocol label switching (MPLS) WAN links to a hub site before being handed off to the Internet. Not only is this scenario expensive, but application performance is often compromised because of WAN bandwidth constraints at the branch and added latency from backhauling connections.

The answer is to use direct internet connectivity to SaaS and trusted web applications from the branch. The right SD-WAN solution makes internet connections secure and reliable by creating encrypted tunnels between every site in the SD-WAN (for inter-branch and branch-to-headquarters traffic), while taking advantage of SSL security provided by the SaaS application for traffic going from the branch to the application directly using the Internet. This hardens the Internet with the security of a virtual private network (VPN), but without the complexity of provisioning and configuring a VPN. With edge-to-edge, encrypted tunnels and a stateful firewall, a secure SD-WAN solution can prevent unauthorized outside traffic from entering the branch.

#2

Apply micro-segmentation for highly granular security

Micro-segmentation—segmenting traffic based on application characteristics, performance requirements, and security policies—is a best practice approach to security, but traditionally difficult to apply in WAN environments. However, with the right SD-WAN solution, you can deploy a fine-grained segmentation approach that extends micro-segmentation from the data center across the WAN to produce a zero-trust architecture.

Granular security controls can be applied to a very small group of resources—for instance, defining a specific set of policies for a particular branch location's use of critical applications such as a customer relationship management (CRM) system, cloud-based applications such as Microsoft Office 365, real-time traffic such as voice over IP (VoIP), and more.

With micro-segmentation, you can improve security by:

- Segmenting and applying distinct policies for each application or group of applications
- Responding quickly to threats to contain and isolate them from other segments
- Automating policy enforcement
- Reducing the attack surface by isolating applications (if one is compromised, other applications are not at risk because they are segmented)
- Gaining greater control and manageability

#2 Apply micro-segmentation for highly granular security

continued

For robust, yet easy-to-manage, micro-segmentation, look for an SD-WAN with:

- Virtual WAN overlays that segment traffic based on business intent, classifying each type of traffic based on application characteristics, service level agreements (SLAs), quality of service (QoS) required, and more, with granular security policies that can be easily applied to groups of applications
- An application whitelist model and stateful firewall that prevent traffic from entering the branch unless it is initiated by users, eliminating unknown traffic from coming into the branch
- Strong encryption, including the ability to encrypt data in-flight, as well as hashing for message integrity

#3

Securely connect branches directly to internet applications

With a sophisticated SD-WAN solution, you can intelligently steer trusted, internet-bound application traffic from the branch directly to the Internet, eliminating inefficient backhauling. However, not all SD-WANs are the same. The difference is the ability to automate the identification of trusted SaaS and web applications that can go directly to the Internet and those that should get backhauled to headquarters for additional security inspection.

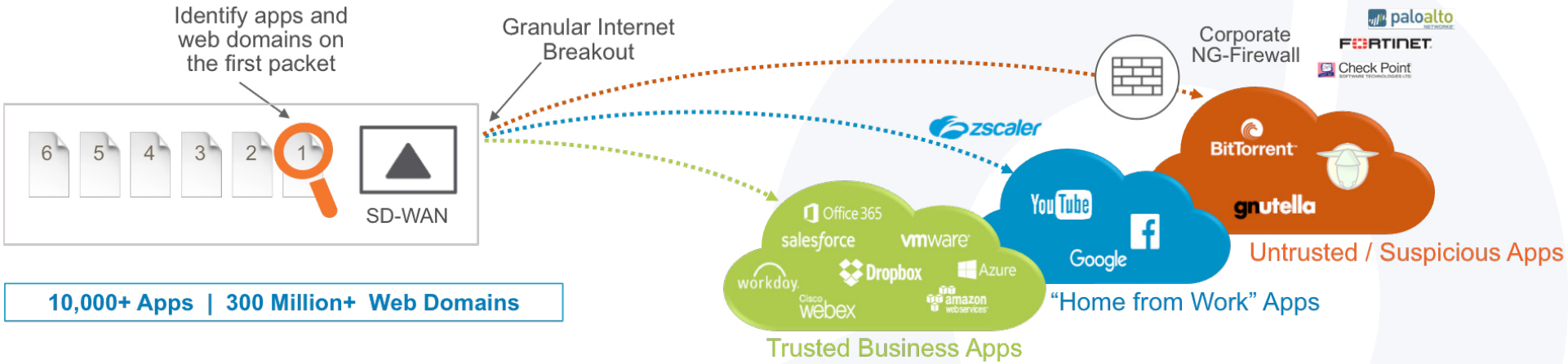
Look for a solution that goes beyond ports and protocols to provide granular application identification based on the first packet received. Traditional, deep packet inspection (DPI)-only approaches require a few packets to identify the application. With multiple application intelligence techniques, including first-packet identification, you gain the ability to granularly direct traffic based on policy: directly to the Internet for trusted traffic, to a secure web gateway for other traffic such as YouTube streaming, or to a headquarters-based next-generation firewall for unknown or suspicious traffic. You can mitigate security risks while enabling the SD-WAN to adapt automatically to changing conditions.

In addition to first-packet identification, you should also look for an SD-WAN solution with a built-in, stateful firewall to ensure that no unauthorized outside traffic can enter the branch, while branch-initiated sessions are allowed.

#3 Securely connect branches directly to internet applications

continued

Figure 1. Granular Internet Breakout for Branches



#4

Make zero-touch provisioning secure

One of the biggest advantages of moving to an SD-WAN solution is zero-touch provisioning, which lets you bring a new branch or remote location online in a matter of minutes, with no specialized IT expertise required at the branch. Zero-touch provisioning also minimizes the risk of human error because a policy is defined (or a change to a policy made) once, then is automatically "pushed" or distributed to all devices in the SD-WAN.

While a boon to the speed and ease with which new branch offices can be added to the WAN, zero-touch provisioning also requires comprehensive security measures. That's why you should insist on an SD-WAN solution that offers:

- A chain of trust enforced through a controller, orchestrator, or certificate authority to authenticate branch devices
- Strong encryption that creates a secure channel to enforce the chain of trust
- Centralized approval and revocation of devices
- Two-factor authentication for greater protection
- The ability to take unauthorized or rogue devices out of the network by dropping all traffic and preventing the download of configuration information

#5

Easily orchestrate application-driven security policies

To achieve the highest levels of security possible, networking and security technologies need to complement each other. One way to do this is called service chaining, which links the SD-WAN with best-of-breed, third-party security solutions. For instance, internet-bound traffic can be service chained to a cloud-based security gateway for Layer 7 inspection and analytics.

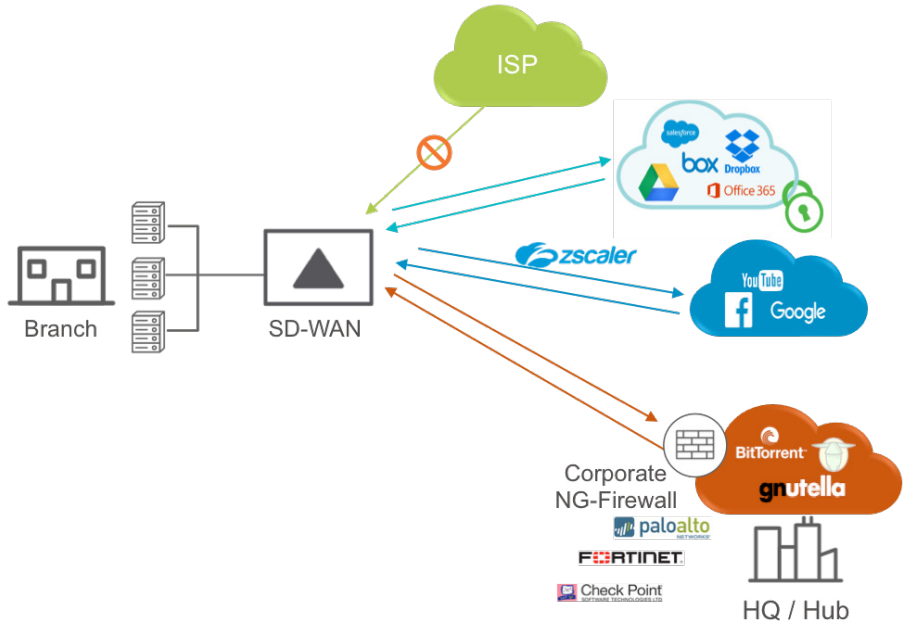
Common service chain examples for SD-WAN environments include:

- **Secure web gateway:** This is used when physical or virtual firewalls are not deployed, e.g. where internet breakout needs to happen close to the egress point, without backhaul.
- **Branch firewall:** While SD-WAN solutions can provide stateful firewall capabilities, for next-generation firewall and other sophisticated Layer 7 inspection, the SD-WAN can be service chained to an on-premise branch firewall.
- **Data center/hub firewall:** Multiple SD-WAN appliances may be service chained to a high-performance firewall at a hub or data center site. This eliminates the requirement for expensive next-generation firewalls at every branch location.

While most SD-WAN solutions let you create service chains, not all of them make it easy to set up and manage. For maximum ease of use, choose an SD-WAN solution with:

- Centralized orchestration and management tools for easy service chaining for local, headquarters, or cloud-based application protection
- Partnerships and technology integrations with leading vendors—such as Check Point, Fortinet, Palo Alto Networks, and Zscaler—for comprehensive security solutions
- Complete automation with a choice of service chaining over multiple links that can balance loads or work in active-backup mode

Figure 2. Service Chaining for Application-Driven Security Policies



#6

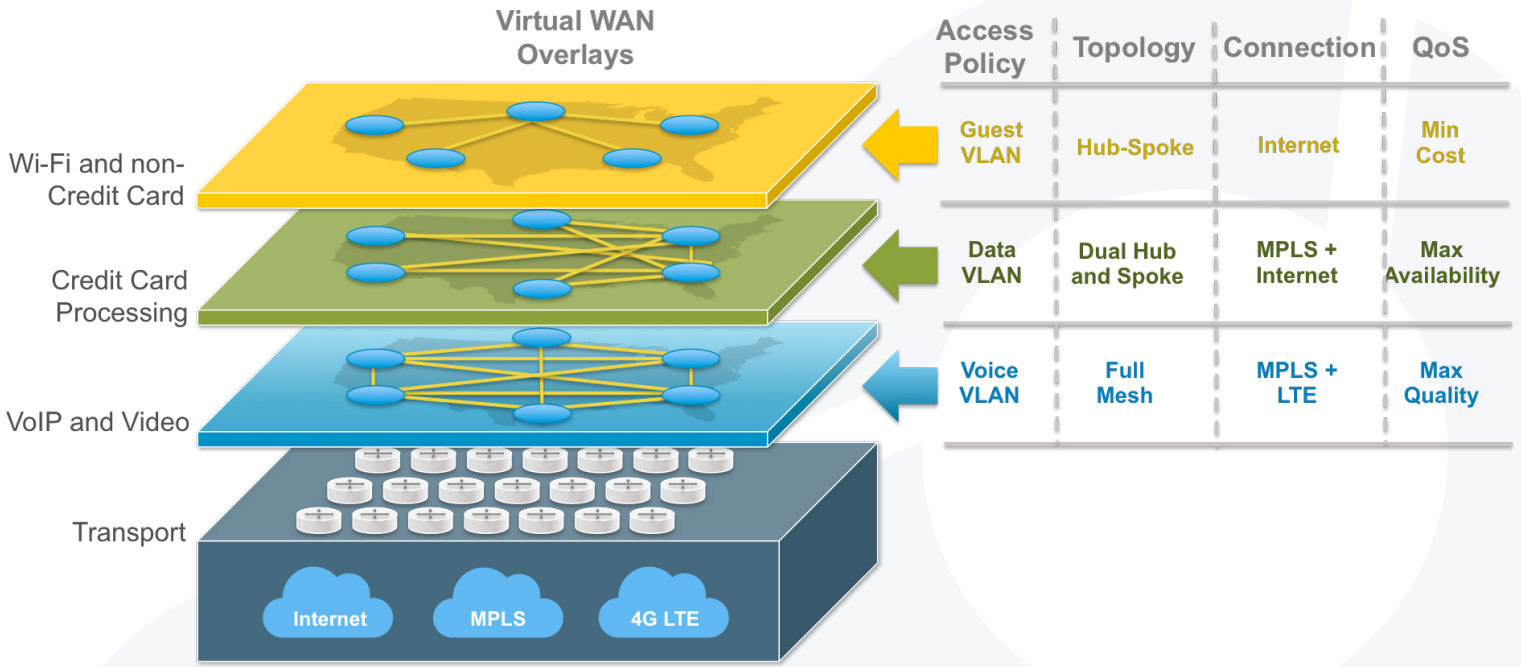
Meet compliance mandates

Whether your company is in a highly regulated industry such as financial services or healthcare, doing business with or for the government, or in an industry that accepts credit card payments, you know the burden of ensuring compliance with relevant industry regulations, including: Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley Act (SOX), and others.

To improve compliance while easing the burden and cost, look for an SD-WAN solution that offers:

- Data plane security with encrypted overlays and micro-segmentation to segment traffic for greater control and reduction of compliance scope. Overlays help isolate traffic to meet compliance mandates—for example, segmenting credit card transactions to comply with PCI DSS
- Control and management-plane security that provides out-of-the-box system security, including: role-based access control, alarms, threshold-crossing alerts, and more
- User authentication, passwords, password controls, roles, and audit logs for change management
- Federal Information Processing Standards (FIPS)-approved security algorithms with correct implementation and failure handling

Figure 3. Virtual WAN Overlays for Compliance



Silver Peak: The industry's most complete SD-WAN solution

Silver Peak SD-WAN solutions enable distributed enterprises to build a better WAN, securely connecting users to applications without compromising application performance, over any WAN transport service. The Unity EdgeConnect SD-WAN solution from Silver Peak addresses all six ways organizations can improve security with features that include:

- **WAN Hardening:** Each WAN overlay is secured and hardened edge-to-edge via 256-bit AES encrypted tunnels. No unauthorized outside traffic can enter the branch. With EdgeConnect, WAN hardening secures branch offices without the appliance sprawl and operating costs of deploying and managing dedicated firewalls.
- **Integrated Stateful Firewall:** An extension of WAN hardening, the integrated stateful firewall allows outbound traffic to exit, but only allows ingress traffic to enter in response to user-initiated sessions, providing robust, branch security. This eliminates the requirement for a separate firewall at branches where no applications are hosted, helping to streamline the WAN architecture.
- **Virtual WAN Overlays:** The EdgeConnect SD-WAN solution is built upon an application-specific, virtual WAN overlay model based on business intent. Multiple virtual overlays abstract the underlying physical transport services and each overlay supports different QoS, transport, and failover characteristics. Virtual WAN overlays also extend micro-segmentation of specific application traffic across the WAN to help maintain security compliance mandates.

- **First-packet iQ:** EdgeConnect uses a unique feature called First-packet iQ that automatically identifies more than 10,000 applications and 300 million web domains based on the first packet received. With granular insight into HTTP/HTTPS traffic, First-packet iQ enables internet breakout automation by steering specific, trusted SaaS and web-based application traffic directly to the Internet while directing unknown or suspicious traffic to a secure web gateway or to a regional hub or data center firewall for further inspection. First-packet iQ utilizes sophisticated techniques to provide the highest levels of application awareness and intelligence available today, helping you meet application SLAs and compliance mandates, while avoiding the use of expensive MPLS bandwidth on non-critical traffic—a major advantage compared to the all-or-nothing traffic approach of other solutions.
- **Secure Zero-Touch Provisioning:** Using a plug-and-play deployment model, EdgeConnect can be deployed at a branch office in seconds, automatically connecting with other Silver Peak instances in the data center, other branches, or in cloud Infrastructure-as-a-Service (IaaS) solutions such as Amazon Web Services, Microsoft Azure, and VMware vCloud Air. By automating the distribution of policy updates, changes, and deletions, Unity Orchestrator (included with EdgeConnect) minimizes human error and reduces potential vulnerabilities.
- **Technology Alliance Leadership:** Industry-leading technology alliances extend the value of the SD-WAN. Silver Peak security partners include: Check Point, Fortinet, Palo Alto Networks, and Zscaler.

Learn more

Download these additional resources to learn more about SD-WAN and security, as well as the Silver Peak Unity EdgeConnect SD-WAN solution:

- Silver Peak EdgeConnect Datasheet
- Silver Peak EdgeConnect Interactive Demo
- Find more information in the Silver Peak resource center

About Silver Peak

Silver Peak is the global leader in broadband and hybrid WAN solutions. Silver Peak offers a high-performance SD-WAN solution that provides secure and reliable virtual overlays to connect users to applications with the flexibility to use any combination of underlying transport without compromising application performance. This results in greater business agility and lower costs. More than 2000 globally distributed enterprises have deployed Silver Peak broadband and hybrid WAN solutions across 80 countries. Learn more at www.silver-peak.com.

© 2017 Silver Peak Systems, Inc. All rights reserved. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners. 04/17